HAAGA-HELIA
ammattikorkeakoulu

IT-jatkuvuussuunnittelu PK-yrityksessä

Timo Huovila

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

15.5.2012

HAAGA-HELIA
ammattikorkeakoulu

Tietotekniikan koulutusohjelma

Tiivistelmä

15.5.2012

Tekijä tai tekijät Timo Huovila.	**Ryhmätunnus tai aloitusvuosi** TIV08
Raportin nimi IT-jatkuvuussuunnittelu PK-yrityksessä	**Sivu- ja liitesivumäärä** 38 + 5
Opettajat tai ohjaajat Heikki Hietala	

Tämä opinnäytetyö kuvaa jatkuvuussuunnitelman laadintaa PK-yrityksen IT-järjestelmille. Jatkuvuussuunnitelman laadinta oli osana yrityksen laajempaa tietoturvasuunnittelua jonka tarkoituksena oli kehittää toiminnan laatua ja valmiutta asiakkaiden erilaisiin vaatimuksiin. Jatkuvuussuunnittelu nähtiin tässä yhteydessä tärkeänä koko yrityksen toimintavarmuutta parantavana toimenpiteenä.

IT-alan yrityksen kyseessä ollessa järjestelmien toimintavarmuus on elinehto yrityksen toiminnalle. Tämän opinnäytetyön tarkoituksena oli luoda jatkuvuussuunnitelmadokumentaatio josta selviää järjestelmiin kohdistuvat riskit, miten niihin on varauduttu etukäteen ja miten realisoituneista uhkista voidaan palautua takaisin normaalitoimintaan.

Opinnäytetyön teoriaosuudessa käydään läpi jatkuvuussuunnittelun käsitteitä ja työvaiheita sekä vaatimuksia joiden pohjalta jatkuvuussuunnitelma tulee laatia.

Opinnäytetyön empiirisessä osassa kuvataan toimintaympäristöä ja itse jatkuvuussuunnitelman laadintaa. Jatkuvuussuunnitelman melko yksilöidyn luonteen vuoksi itse valmista produktia ei esitellä tässä opinnäytetyössä vaan tekstissä ja liitteissä esitellään käytettyjä arviointi- ja koostepohjia sekä joitain yleisiä esimerkkejä tehdyistä toimenpiteistä ja dokumenteista.

Asiasanat
Jatkuvuus, toipuminen, suunnitelma, varautuminen, riskit, tietoturva

HAAGA-HELIA
University of Applied Sciences

Degree Programme in Information Technology

Abstract

15.5.2012

Authors Timo Huovila	**Group or year of entry** TIV08
The title of thesis IT continuity planning for a small business	**Number of pages and appendices** 38 + 5
Supervisor(s) Heikki Hietala	

This thesis describes the creation of continuity planning for the IT infrastructure of a small business. The creation of continuity planning was a part of the company's broader IT security planning which was to improve the quality of functions and preparedness for different customer requirements. In this context continuity planning was seen as an important measure to improve the company's reliability

In the case of an IT company, the reliability of all systems is a key issue for functionality. This thesis was to create documentation of continuity planning, describing risks threatening the systems, how they are prepared for and how to recover from realized threats.

The theoretical part of this thesis consists the concepts as well the steps and requirements for continuity planning.

The empirical part describes the company and IT-environment as well as the process of creating the continuity planning. Because of the detailed nature of the plan, the product itself is not presented in this thesis, but the text and appendix consist of the assessment and compilation templates along with some general examples of completed actions and documents.

Key words
Continuity, recovery, planning, preparing, risk, security

Sisällys

1 Johdanto

IT-järjestelmät ovat nykypäivänä yhä useamman yrityksen toiminnan selkäranka. Erityisesti IT-alalla yritykset ovat erittäin riippuvaisia järjestelmien toimintavakaudesta ja hallitsemattomat käyttökatkokset kriittisissä järjestelmissä saattavat pahimmillaan osoittautua tuhoisiksi yrityksen toiminnalle. Yrityksen IT-järjestelmiä uhkaavien riskien, niiden luokittelu ja kartoitus sekä realisoitumisiin valmistautuminen ja palautumisen suunnittelu onkin erittäin tärkeää häiriötilanteiden vaikutusten minimoimiseksi.

Jatkuvuussuunnitteluprosessin tarkoituksena on mahdollistaa yrityksen toiminnan jatkuminen niin normaalioloissa, häiriötilanteissa kuin myös poikkeusoloissa. Jatkuvuussuunnittelu tuo yritykselle lisäarvoa myös olemalla osana tietoturvallisuutta ja laadunvarmistusta. Toimivalla ja testatulla jatkuvuussuunnitelmalla voidaan merkittävästi vähentää yritykseen kohdistuvia uhkia ja riskejä jo etukäteen sekä huomattavasti säästää aikaa ja resursseja häiriötilanteista palautumisessa.

Yrityksen IT-järjestelmien rakentajana ja niistä vastuullisena jatkuvuussuunnitelman luominen osui luontevasti vastuualueelleni. Koska yritys on varsin nuori ja rakennusvaiheessa ei varsinaiseen jatkuvuussuunnittelun dokumentointiin ollut ehditty paneutumaan, oli opinnäytetyön aiheelle selkeä tilaus yrityksessä. Itse opinnäytetyön teoriaosuus kattaa tutkimustietoa yritysten IT-järjestelmien kohtaamista riskeistä ja niihin varautumisesta, jatkuvuussuunnittelun käsitteistä ja prosessista sekä siihen liittyvistä standardeista ja erilaisista malleista. Empiriaosuudessa kuvataan toimintaympäristöä, jatkuvuussuunnittelussa läpikäytyjä työvaiheita sekä tehtyjä varautumistoimenpiteitä.

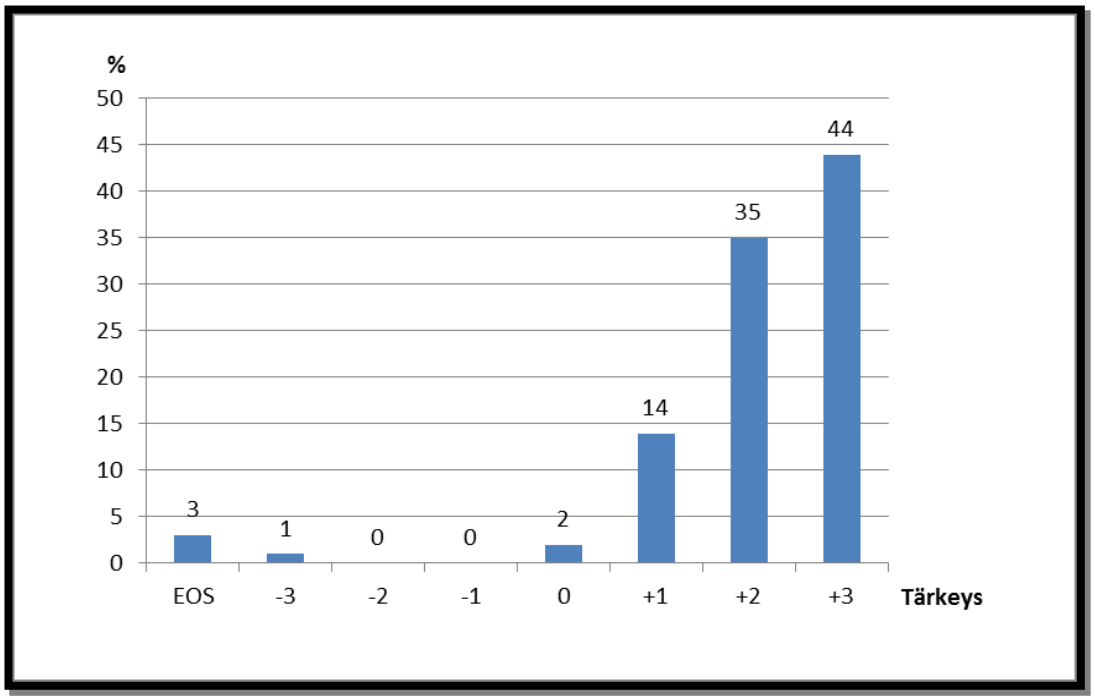
1.1 Tutkimusongelma ja rajaus

Osana laajempaa tietoturvan kehittämishanketta Yritys X:ssä otettiin laadittavaksi jatkuvuussuunnitelma toiminnan jatkuvuuden takaamiseksi, häiriötilanteiden estämiseksi ja niistä toipumiseksi. Tämän opinnäytetyön tarkoituksena on kartoittaa Yritys X:n IT-järjestelmien uhkia sekä riskejä, miten näihin on varauduttu ja luoda malleja mahdollisista häiriötilanteista palautumiseen. Tavoitteena on luoda dokumentaatiopohjat ja käytännöt riskien arviointiin, niiltä suojautumiseen ja vikatilanteista palautumiseen.

Opinnäytetyö rajataan koskemaan yrityksen käyttämien palveluiden ja palvelimien fyysisiä taustajärjestelmiä, jotka kaatuessaan tai vahingoittuessaan aiheuttaisivat häiriötä kaikkiin yrityksen palvelimiin, prosesseihin ja toimintoihin, joten tarkempia prosessien keskeytysanalyyseja ei tämän opinnäytetyön puitteissa tehdä. Syntyneeseen jatkuvuussuunnitelmaan kirjataan seuraavaan versioon sisällytettävät jatkotutkimukset ja analyysit.

2 Tutkimustietoa

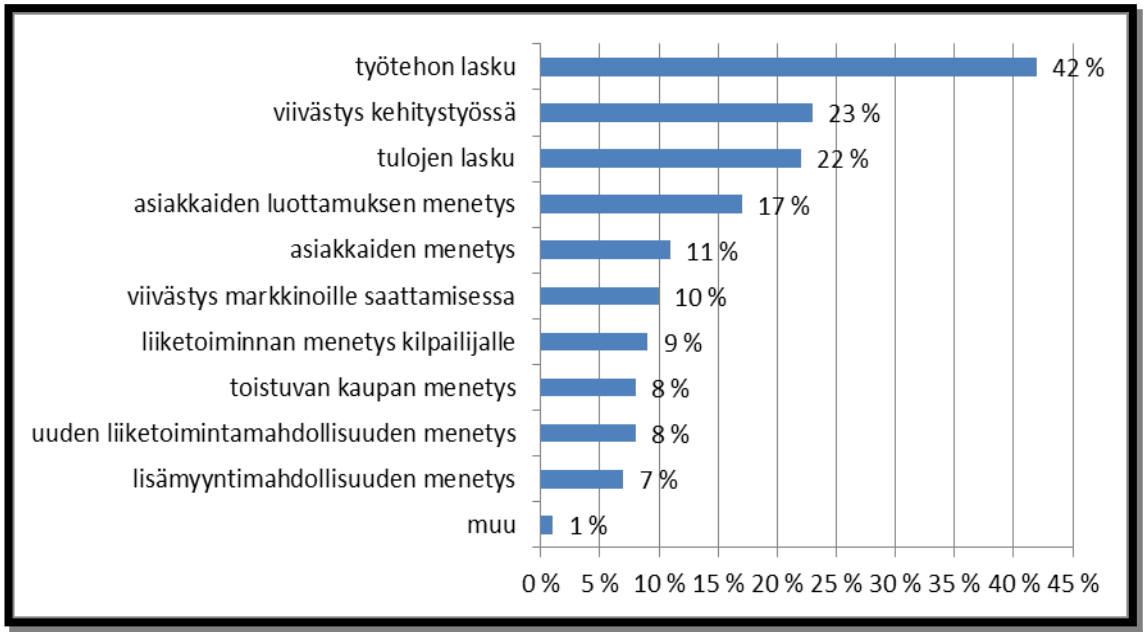
IT-järjestelmien toimivuuden merkitystä nykypäivän yritysten toiminnassa ei voi liialti korostaa. Tietotekniikan liiton, Symantecin ja Rittalin Suomessa vuonna 2007 suorittaman pk-yritysten tietoturvatilannetutkimuksen mukaan valtaosa tutkituista yrityksistä kokee IT-infrastruktuurin erittäin merkittäväksi tekijäksi toimintaympäristössään. Kuviossa 1 on kuvattu yritysten näkemys IT-infrastruktuurinsa merkityksestä asteikolla -3 - +3.



Kuvio 1. IT-infrastruktuurin merkitys yritykselle (Tietotekniikan liitto 2007, 4)

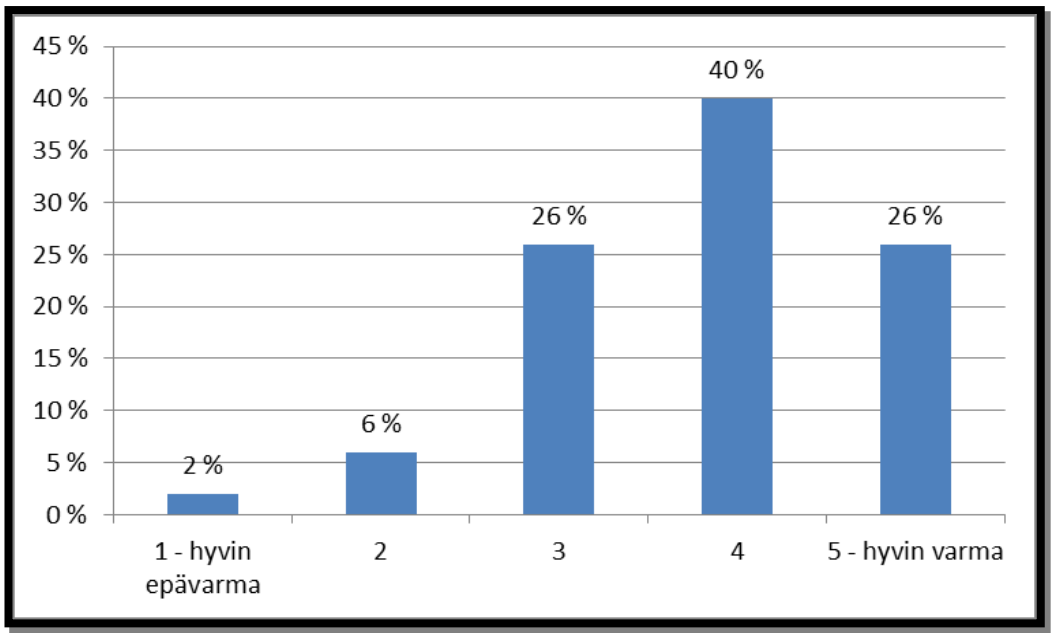
Saman tutkimuksen mukaan 94 % yrityksistä käytti jonkinlaista varmuuskopiointiratkaisua mutta vain 9 % suoritti säännöllisiä palautustestauksia.

EMC Corporation julkaisi marraskuussa 2011 tutkimuksen eurooppalaisten yritysten varautumis- ja palautumissuunnitelmista IT-katastrofin osuessa kohdalle. Tutkimukseen osallistuneista yrityksistä 47 % oli kokenut katkoja IT-järjestelmissään viimeisen 12 kuukauden aikana (EMC 2011, 31). Yleisimmäksi katkojen aiheuttamista haittatekijöistä nousi selkeästi työtehon lasku, jonka oli kokenut 42 % IT-järjestelmissään häiriöitä kohdanneista yrityksistä, kuten voidaan todeta kuviosta 2.



Kuvio 2. IT-järjestelmien katkojen seuraukset (EMC 2011, 35-37)

Samassa tutkimuksessa kysyttiin myös yritysten luottamusta palautumismahdollisuuksiinsa katastrofin sattuessa. Vain 8 % yrityksistä koki epävarmuutta palautumiskykynsä suhteen kuten on esitetty kuviossa 3.



Kuvio 3. Yritysten luottamus palautumiskykyynsä IT-katastrofin sattuessa (EMC 2011, 83-85)

Tutkimuksesta voidaan siis päätellä että yritykset ymmärtävät hyvin sekä IT-järjestelmien että niihin kohdistuvien katkosten ja häiriöiden merkityksen liiketoiminnalleen. Täten myös järjestelmien jatkuvuuteen ja palautumiskykyyn osataan suurimmilta osin suhtautua riittävällä vakavuudella ja resursseilla liiketoiminnan häiriöiden minimoimiseksi.

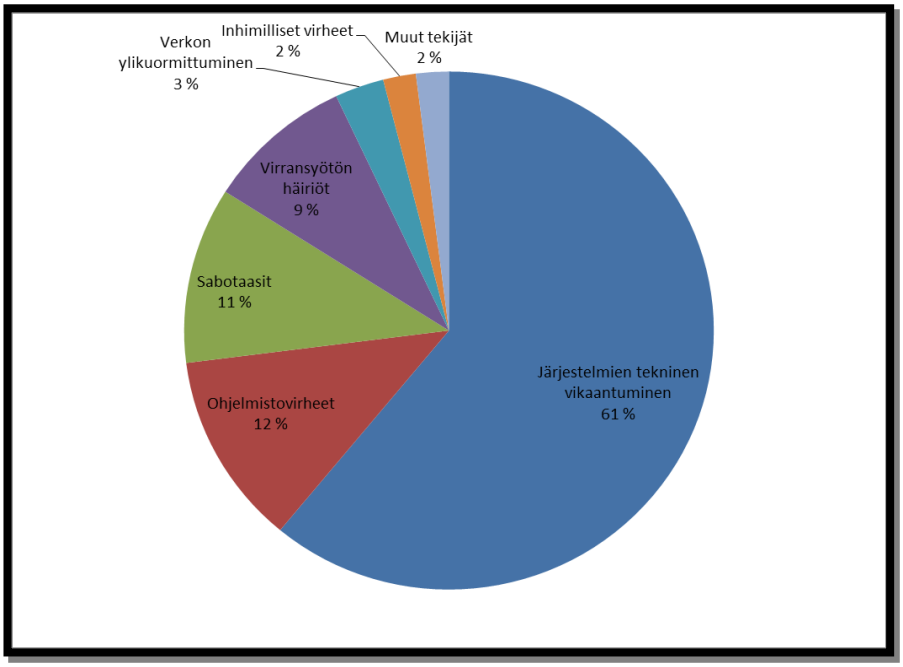
3 Riskit

”IT-riski on jokin asia, jossa tietotekniikka voi epäonnistua ja joka vaikuttaa liiketoimintaan negatiivisesti.” (Jordan & Silcock 2006, 58)

Tietojärjestelmien riskit koostuvat erilaisista uhkista jotka voivat aiheuttaa järjestelmiin vikoja, tiedon katoamista tai tiedon muuttumista. Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) julkaisema Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa(2003, 33–35) listaa tietojärjestelmien uhkia seuraavasti:

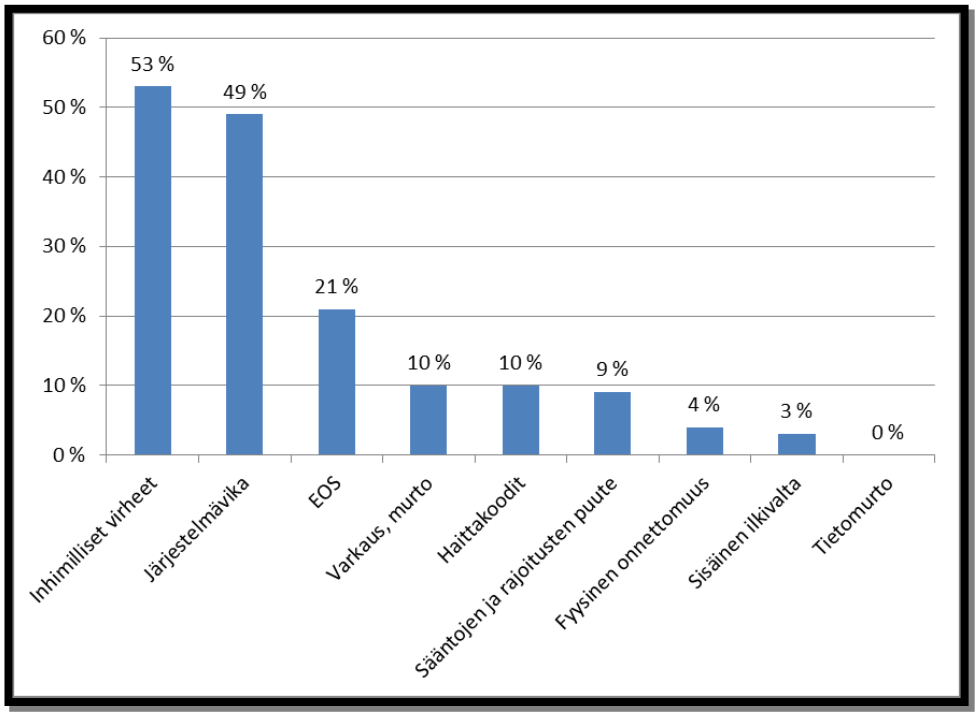
- puutteelliset toimintatavat, esim. dokumentaation ja ohjeistuksen puutteet
- tahattomat teot, esim. inhimilliset virheet, kokemattomuus
- tekniset viat, esim. tietoliikennehäiriöt, laiterikot
- tahalliset teot, esim. hyökkäykset, ilkivalta
- ylivoimainen este, esim. tulipalo, vesivahinko

Yleisimpien uhkien jakautuminen vaihtelee hieman tutkimuksittain, mutta esim. PriceWaterhouseCoopersin v. 2006 julkaiseman tutkimuksen mukaan järjestelmien tekninen vikaantuminen on syynä 61 %:ssa tapahtumista jotka johtavat toimintakatkoihin tai datan korruptoitumiseen. Tutkimuksen tulokset on kuvattu tarkemmin kuviossa 4.



Kuvio 4. syyt toimintakatkoihin tai datan korruptoitumiseen ((Laaksonen, Nevasalo & Tomula 2006. 2006, s. 230)

Tietotekniikan liiton teettämässä kotimaisten pk-yritysten tietoturvatutkimuksessa suurimmaksi datan katoamisen syyksi nousivat puolestaan inhimilliset virheet 53 %:n osuudella, järjestelmävikojen jäädessä toiselle sijalle 49 %:n osuudella.



Kuvio 5. Suurimmat tietojen katoamisten syyt (Tietotekniikan liitto 2007, 12)

Vaikka tutkimusten kysymyksenasettelut ja täten myös tulokset eroavat toisistaan, voidaan kuitenkin päätellä että yrityksien IT-järjestelmien suurimmat uhat tulevat oman talon sisältä. Ihmisten, laitteiden ja ohjelmistojen virheet ja häiriöt ovat ylivoimaisessa enemmistössä katkoksissa ja tapauksissa jotka johtavat tietojen menetykseen. PriceWaterHouseCoopersin tutkimuksessa 75 % tapauksista johtui sisäisistä tekijöistä, Tietotekniikan liiton tutkimuksen mukaan taas puolet haastatelluista yrityksistä koki inhimilliset virheet ja järjestelmäviat suurimpina tiedon katoamisen aiheuttajina. Julkisuudessa eniten palstatilaa saavat ulkoapäin tapahtuvat häiriö- ja vahinkotekijät kuten virukset, palvelunestohyökkäykset, fyysiset murrot ja ilkivalta jne. olivat molemmissa tutkimuksissa edustettuna vain n. 10 %:ssa tapauksista.

4 Jatkuvuussuunnittelu

Jatkuvuussuunnittelun tarkoituksena voidaan pitää yllättäviin tilanteisiin valmistautumista ja reagoinnin helpottamista poikkeustilanteissa ja – oloissa. Jatkuvuussuunnittelu tulisi käsittää ennen kaikkea prosessina joka tuo mukanaan testatut ja ylläpidetyt jatkuvuus- ja palautumissuunnitelmat, tietouden yrityksen järjestelmien ja prosessien prioriteeteista ja kyvyn ylläpitää, suojata ja palauttaa näiden toimintoja sekä järjestelmiä tärkeysarvonsa mukaan. Etenkin IT-alan vahvasti teknologiapohjaisessa toiminnassa on tärkeää tunnistaa kriittisimmät palvelut ja järjestelmät joiden vikaantuminen saattaisi aiheuttaa koko toiminnan halvaantumisen.

Tämä opinnäytetyö keskittyy ensisijaisesti yrityksen IT-järjestelmien jatkuvuussuunnitteluun: poikkeustilanteiden havainnointiin, ennaltaehkäisyyn ja tilanteista palautumiseen.

4.1 Jatkuvuussuunnittelun käsitteet

Jatkuvuussuunnittelu

Jatkuvuussuunnittelu on prosessi jolla varaudutaan toimintojen ja jatkuvuuden ylläpitämiseen normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa (Iivari & Laaksonen 2009, 18). Jatkuvuussuunnittelu ei suinkaan ole kertaluontoinen projekti vaan jatkuva prosessi jonka ajantasaisuutta ja toimivuutta tulee ylläpitää ja testata. Jatkuvuussuunnittelu pitää sisällään myös estotoimenpiteitä joilla pyritään estämään riskien realisoitumista, sekä havainnointivälineitä joilla pyritään havaitsemaan mahdolliset häiriötilanteet jo ennen poikkeustilanteeseen ajautumista.

Toipumissuunnitelma

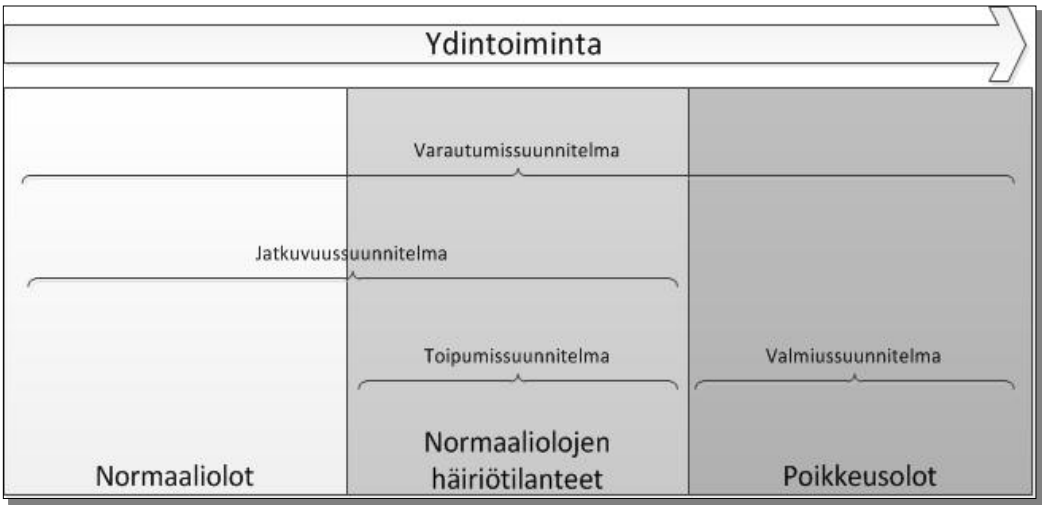
Toipumissuunnitelma on osa jatkuvuussuunnittelua, tarkoituksena suunnitella toimenpiteet joilla riskien realisoituessa poikkeustilanteeksi saadaan tilanne normalisoitua ja haitat minimoitua. Suunnitelma on aikajänteeltään lyhyt kirjallinen ja prosessi- tai järjestelmäkohtainen toimenpideohjeistus, ts. sisältää toimenpiteet yksittäisten liiketoimintaprosessien osien palauttamiseen. Suunnitelmien tulee olla poikkeustilanteessa helposti saatavilla, tulkittavissa ja toteutettavissa, myös painetilanteessa.

Valmiussuunnittelu

Etenkin julkishallinnossa käytetty valmiussuunnittelun käsite ei ole täysin vakiintunut, mutta käsittää yleisesti ottaen kuvauksen toimenpiteistä joiden avulla toimintaa voidaan jatkaa vakavissa häiriötilanteissa ja poikkeusoloissa kuten esim. sota-aikana (Iivari & Laaksonen 2009, s. 20). Valmiussuunnittelu koskee ensisijaisesti tärkeysluokiteltuja organisaatioita joilla on merkittävä rooli yhteiskunnan toimivuuden kannalta poikkeusoloissa.

Varautumissuunnittelu

Varautumissuunnittelun voidaan katsoa pitävän sisällään kaikki edellä mainitut osiot. Varautumissuunnitelma kattaa siis niin normaaliolojen poikkeustilanteet ja niihin valmistautumisen ja toipumisen, kuin myös poikkeusoloissa toiminnan jatkuvuuden mahdollistamisen vaativat toimenpiteet ja käytännöt. Kuviossa 6. on tiivistettynä jatkuvuussuunnittelun käsitteet ja suhteet toisiinsa.



Kuvio 6. Jatkuvuussuunnitelman, toipumissuunnitelman, valmiussuunnitelman ja varautumissuunnitelman suhde (Iivari & Laaksonen 2009, 19)

4.2 Standardit ja apuvälineet

Jatkuvuussuunnittelussa on hyvä käyttää apuna valmiita standardeja ja toimintamalleja, jotka tarjoavat laajalti pohditun, selkeän ja vertailukelpoisen rakenteen pohjatyölle ja dokumentoinnille (Hakala, Vainio & Vuorinen 2006, 46). Iivari & Laaksosen mukaan (2009, 82) IT-jatkuvuussuunnittelun standardointi laahaa kuitenkin vielä hieman muita hallintajärjestelmien standardointeja perässä, ja ovatkin lähinnä osana yleisempiä tietoturva- tai yrityksen jatkuvuushallinnan standardeja. Standardit eivät yleisesti ottaen ole vapaasti saatavilla, vaan ovat ostettavissa standardoinnin laatineelta järjestöltä.

Jatkuvuussuunnittelua käsitteleviä tai sisältäviä standardeja ovat ainakin British Standard Instituten (BSI) luoma BS 25999-sarja joka käsittelee liiketoiminnan jatkuvuussuunnittelun käytäntöjä. ISO 27000-sarja käsittelee yritysten tietoturvaa laajemmin ja sarjan numero 27031 on varattu jatkuvuudenhallinnalle mutta standardin sisällöstä ei ole vielä virallista näkemystä eikä täten edes laadittavana (Iivari & Laaksonen 2009, 87).

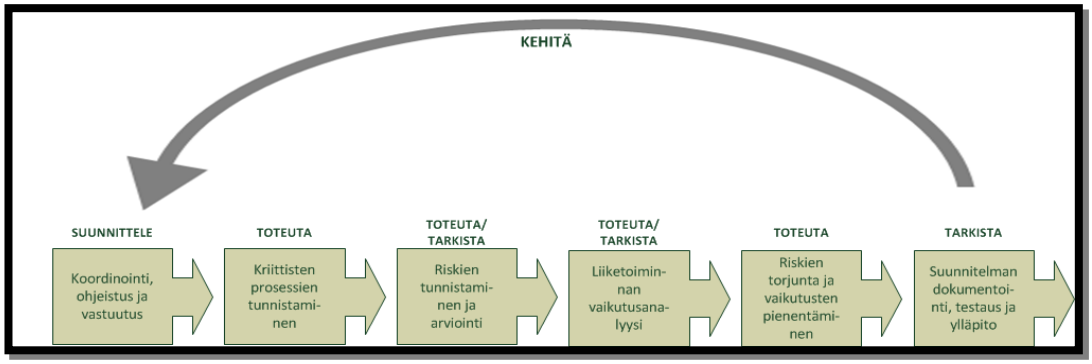
Riskianalyysien tekoon on myös luotu apuvälineitä ja työkaluja. Kotimainen Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) vuonna 2003 julkaisema Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa sisältää valtion tietoturvallisuuden linjauksia ja ohjeita sekä riskien arviointiin apuvälineitä ja menetelmiä jotka soveltuvat käyttöön myös yritysmaailmassa. Kansainvälisistä standardeista

ISO27005:2008:n liitteissä löytyy ohjeita ja taulukoita uhkien, haavoittuvuuksien sekä järjestelmien luokitteluun.

5 Jatkuvuussuunnittelun työvaiheet

Jatkuvuussuunnitteluprosessin laadinta ja työmäärä ovat luonnollisesti riippuvaisia kohdeyrityksestä, sen toimintamalleista ja – ympäristöstä (Laaksonen ym. 2006, s. 230–231). Kuviossa 7 on esitelty jatkuvuussuunnittelun jatkuvan prosessin työvaiheet (Iivari & Laaksonen 2009, s. 93):

- suunnittelun koordinointi ja vastuiden määrittely
- kriittisten prosessien tunnistaminen ja kuvaaminen
- prosessien riskianalyysit
- vaikutusanalyysi
- riskien torjunta ja vaikutusten pienentäminen jatkuvuus- ja toipumis-suunnitelmilla
- suunnitelmien dokumentointi, testaus ja ylläpito.



Kuvio 7. Jatkuvuussuunnittelun vaiheet (Iivari & Laaksonen 2009, 93)

5.1 Suunnittelun koordinointi, vastuutus ja ohjeistus

Jatkuvussuunnnittelu lähtee suunnittelun koordinoinnista ja vastuutuksista, yrityksestä valitaan henkilöt tai työryhmät joille jaetaan tehtävät suunnitelman laatimiseksi, ylläpitämiseksi ja testaamiseksi. IT-jatkuvuussuunnittelussa pääpaino on luonnollisesti IT-henkilöstöllä mutta myös johdon ja käyttäjien osallistumista tarvitaan jotta suunnitelma tukee myös liiketoiminnan prosesseja eikä ajaudu nojautumaan liiaksi pelkkiin teknisiin ratkaisuihin.

Ensimmäisessä vaiheessa jatkuvuus- ja toipumissuunnitelmille suunnitellaan myös yhtenäinen rakenne ja mallipohjat joiden mukaan dokumentointi suoritetaan. Dokumentaation ja suunnittelun ohjeistuksena ja pohjina voidaan käyttää standardeja ja muita yleisesti hyväksi havaittuja malleja (Iivari & Laaksonen 2009, 97). Ensimmäisen vaiheen tavoitteena on varmistua seuraavista asioista (Iivari & Laaksonen 2009, 97):

- suunnitelmien yhtenäisyys
- suunnitelmat liittyvät toisiinsa ja tukevat toisiaan
- kokonaisuus on yhden tason hallinnassa ja ohjauksessa
- suunnittelijoilla on konkreettista apua saatavissaan ja tietävät mistä apua saadaan
- suunnittelutyö on tehokasta

5.2 Kriittisten prosessien tunnistaminen ja kuvaaminen

Jatkuvuussuunnittelun toinen vaihe käsittää yrityksen kriittisten prosessien tunnistamisen ja kuvaamisen. Yhdessä johdon kanssa käydään läpi yrityksen toiminnan prosessit ja näiden omistajat sekä arvioidaan toiminnan kannalta kriittisimmät prosessit joiden pidempiaikainen häiriintyminen toisi vakavaa haittaa liiketoiminnalle.

Prosessien kuvaukseen liittyy myös prosessien riippuvuudet eri tuotannontekijöistä, eritoten niihin liittyvät tietojärjestelmät (Iivari & Laaksonen 2009, 106, 114) IT-henkilöstön tulee selvittää prosessien kannalta tärkeimmät järjestelmät joiden vioittuminen voisi johtaa prosessien vikaantumiseen tai täydelliseen halvautumiseen ja sitä myötä liiketoiminnan häiriöihin.

5.3 Riskien tunnistaminen ja arviointi

Kriittisten prosessien ja järjestelmien tunnistamisen jälkeen tulee näille tehdä riskikartoitus jossa haetaan potentiaalisia riskejä jotka voidaan katsoa mahdollisesti tapahtuviksi suunnitelman piiriin kuuluvissa järjestelmissä. Riskianalyysi voidaan tehdä vaiheittaisesti aloittaen yleisemmän tason riskikartoituksesta jonka avulla etsitään yleisluontoisempia riskejä jotka voivat uhata mitä tahansa yrityksen järjestelmiä. Yhteisten riskien selvityksen jälkeen voidaan siirtyä kartoittamaan yksityiskohtaisempia riskejä yksittäisistä järjestelmistä.

Riskien selvityksen jälkeen riskit tulee arvioida. Riskien arvioinnissa voidaan käyttää taulukkoa johon riskit eritellään ja luokitellaan eri määreiden kuten esim. vakavuuden ja todennäköisyyden perusteella. Mitä vakavampi ja todennäköisempi riskin toteutuminen on, sitä enemmän siihen on varauduttava (Hakala ym. 2006, s. 81). Riskien selvityksen ja arvioinnin tuloksena saadaan selville olemassa olevat riskit ja näiden merkittävyys liiketoiminnalle

5.4 Vaikutusanalyysi

Vaikutusanalyysi on vahvasti sidoksissa riskianalyysiin. Vaikutusanalyysillä pyritään selvittämään järjestelmien häiriötilanteiden vaikutus tukemiinsa prosesseihin ja liiketoimintaan, mitä häiriöt kustantavat riippuen häiriön pituudesta ja millaisella panostuksella häiriöihin tulee varautua.

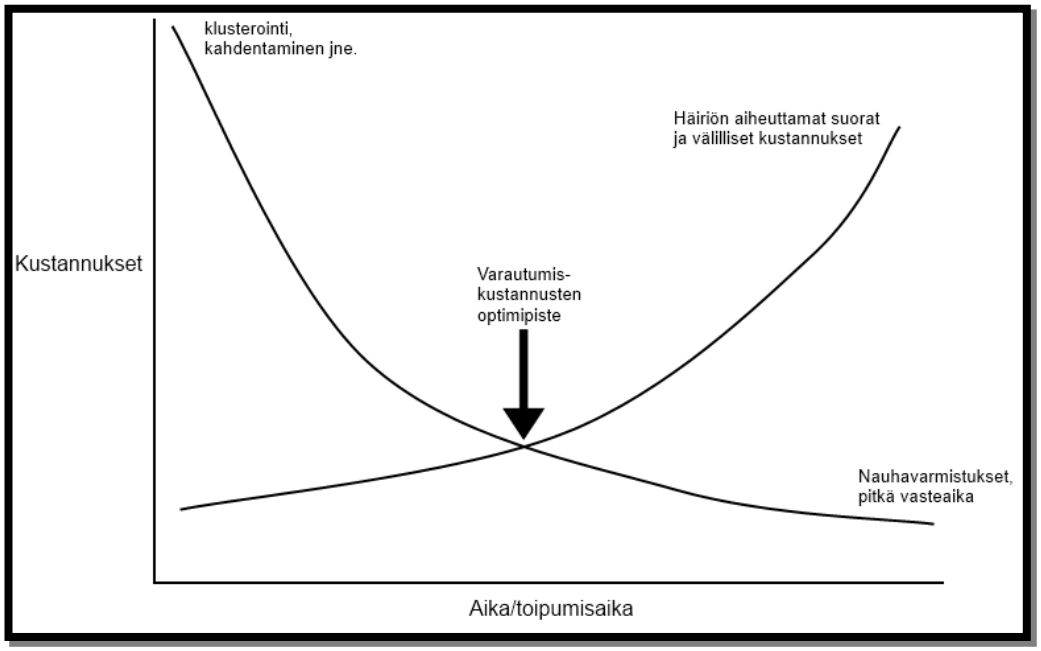
Vaikutusanalyysillä tulisi selvittää ainakin seuraavat asiat (Laaksonen ym. 2006, 233):

- identifioitujen riskien toteutumisen aiheuttamat kustannukset ja siedettävä enimmäiskatkoaika
- riskien toteutumisen laajuus
- haitta tuotannolle, myynnille, maineelle
- vaihtoehdot jatkuvuuden parantamiseksi tai toipumiseksi

5.5 Riskien torjunta ja vaikutusten pienentäminen

Tärkeä osa jatkuvuussuunnittelua riskien tunnistamisen jälkeen on luoda ennakoivia ja valvovia käytäntöjä todennäköisimpien ja torjuttavissa olevien riskien realisoitumisen ehkäisemiseksi. Riskien torjuntaa suunnitellessa tulee ottaa huomioon mahdollisen torjuttavissa olevan riskin kustannusvaikutus riskin realisoituessa ja verrata sitä riskin torjunnan vaatimiin kustannuksiin. Yleisesti ottaen häiriön kustannukset kasvavat mitä pidempään mahdollinen häiriötilanne jatkuu ja toisaalta vastaavasti häiriön estäminen tai vaikutusten minimointi ja järjestelmien palauttaminen kustantaa sitä enemmän mitä pikemmin asiaan voidaan puuttua. Mitä kauemmin toiminta kestää häiriötilannetta, sitä pienemmillä kustannuksilla voidaan tilanne torjua tai palauttaa. Riskin torjunnan ja mahdollisen häiriötilanteen kustannuksia verrataan toisiinsa ja valitaan varautumis- tai

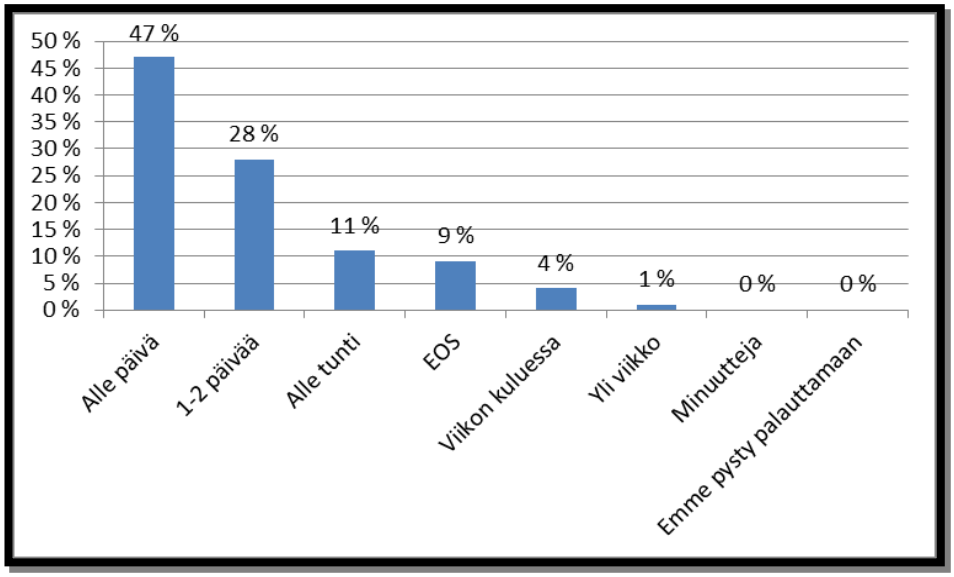
palautumistapa joka on kustannuksiltaan oikeassa suhteessa häiriötilanteen aiheuttamiin kustannuksiin, kuten kuviossa 8 on esitetty.



Kuvio 8. Riskien torjunnan kustannusvaikutusanalyysi (Iivari & Laaksonen 2009, 144)

Riskejä kuitenkin harvoin pystytään kokonaisuudessaan poistamaan tai välttämään. Hakala ym. (2006, s. 92) kuvaavat turvallisuutta parantavan keinon käyttöönoton jälkeen jäävää riskiä jäännösriskiksi, joka ei saa olla hyväksyttävää riskiä suurempi. Jäännösriski tulee myös dokumentoida jatkuvuussuunnitelmiin.

Kuviossa 9 on kuvattu Tietotekniikan liiton kyselyyn osallistuneiden yritysten arvioita kriittisen palvelimen tietojen palauttamiseen kuluvasta ajasta.



Kuvio 9. Kriittisen palvelimen tietojen palauttamiseen kuluva aika (Tietotekniikan liitto 2007, 4)

Tuloksista nähdään että kaikilla yrityksillä on jonkinlainen palautumissuunnitelma olemassa IT-järjestelmiensä suhteen mutta palautumisajan suhteen joudutaan tekemään kompromisseja: yhdenkään yrityksen mukaan ei ollut mahdollista palauttaa tietoja minuuteissa, mutta toisaalta yhdessäkään yrityksessä ei koettu palautumista täysin mahdottomaksi. Mitä lyhyempi on palautumisaika, sitä korkeammat ovat kustannukset. Suurimmalla osalla palautuminen on mahdollista skaalalla alle päivä – 1-2 päivää joka koetaan hyväksyttäväksi jäännösriskiksi

5.6 Suunnitelmien dokumentointi, testaus ja ylläpito

Kun edellä mainitut toimenpiteet on saatu suoritettua, tulee tulokset koostaa alussa luotujen dokumenttipohjien mukaan yhteneväiseksi dokumentaatioksi sekä laatia toipumis-, testaus- sekä ylläpitosuunnitelmat jatkuvuussuunnitelman ajantasaisuuden ja relevanssin takaamiseksi. Parhaastakaan jatkuvuussuunnitelmasta ei kuitenkaan ole apua jos suunnitelmaa ei testata tai päivitetä joten testaus- ja päivityssuunnitelmien ja -rutiinien teko kuuluu olennaisena osana jatkuvuussuunnitteluprosessiin.

Suunnitelmien saavutettavuus on myös erittäin tärkeä huomioonotettava seikka ja Iivari & Laaksonen(2009, s. 158) muistuttavatkin että dokumentit tulee säilyttää niin digitaalisesti kuin paperilla ja ehdottomasti vähintään kahdessa fyysisesti erillisessä paikassa. Säilytyksessä tulee ottaa huomioon niin tietoturvaseikat kuin myös helppo saavutetta-

vuus mahdollisen häiriötilanteen sattuessa. Dokumenttien päivityksen yhteydessä kaikki kopiot tulee luonnollisesti niin ikään päivittää ajantasaisiksi.

6 Taustaa

Yritys X on suomalainen, vuonna 2011 perustettu ohjelmistojen suunnitteluun ja valmistukseen keskittynyt yritys joka toimittaa asiakkailleen helppokäyttöisiä verkkopalveluita. Yrityksellä on yksi toimipiste Helsingissä, joka työllistää kirjoitushetkellä 15 henkilöä. Yritys on itsenäisessä muodossaan varsin nuori johtuen kesällä 2011 loppuunsaatetuista yritysjärjestelyistä joiden seurauksena Yritys X irtautui entisestä Yritys Y:stä, mutta historiaa ja kokemusta yrityksellä ja sen työntekijöillä on alalta runsaasti, ulottuen aina 1990-luvun alkupuolelle saakka.

Yritys X irtautui 1.8.2011 Yritys Y:stä omaksi yrityksekseen, jonka seurauksena syntyneelle yritykselle piti rakentaa kokonaan oma IT-infrastruktuurinsa. Alan, sekä osin asiakkaiden vaatimusten myötä infrastruktuuria rakentaessa ei voitu tukeutua julkisiin pilvipalveluihin, vaan katsottiin asianmukaisimmaksi pitää yrityksen sisäiset laitteistot ja informaatio kokonaisuudessaan oman talon sisällä.

Infrastruktuuri pyrittiin alusta alkaen rakentamaan täyttämään PK-yritykselle riittävän saavutettavuuden ja jatkuvuuden tason kustannusrealiteetit huomioon ottaen. Itse jatkuvuus- ja palautumissuunnittelun dokumentointi kuitenkin jäi järjestelmää rakennettaessa myöhempään vaiheeseen rakennusvaiheen resursseista johtuen, jota aukkoa paikkaamaan tämä opinnäytetyö on otettu tehtäväksi.

6.1 Järjestelmät

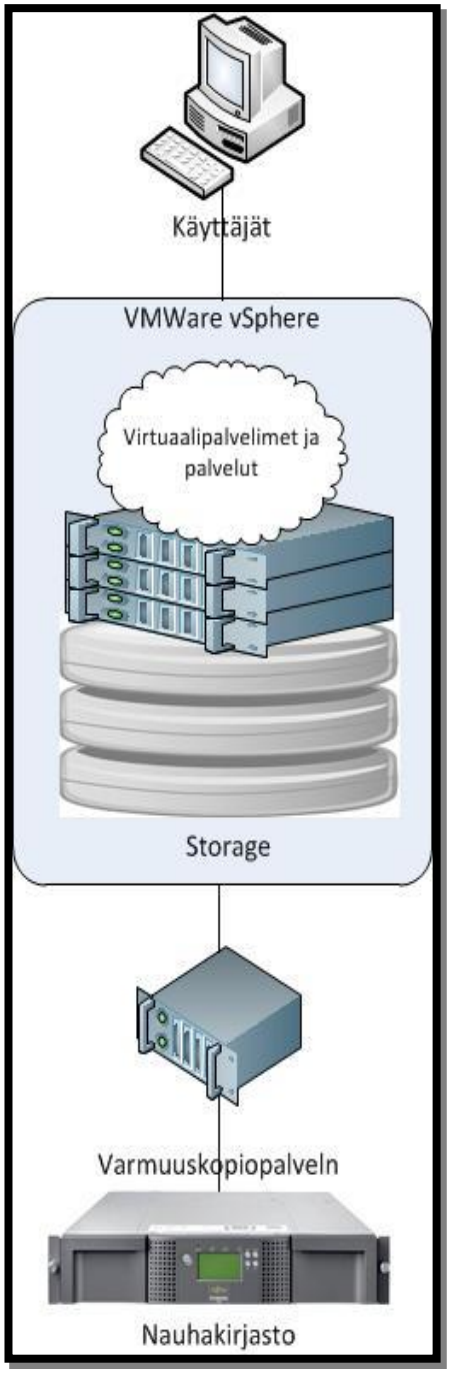
Yritys X:n IT-infrastruktuuri on rakennettu lähes kokonaan virtuaaliympäristön varaan. Virtualisoitu palvelinympäristö tuo mukanaan monia etuja ei pelkästään jatkuvuuden vaan myös joustavuuden ja käytettävyyden kannalta. Lisäksi tarpeena oli säilyttää yhteensopivuus taakse jääneen yrityksen infrastruktuurin kanssa, toistaiseksi osittaisesti yhteisten järjestelmien myötä.

Tässä luvussa käydään läpi infrastruktuurin laitteistot ja ohjelmistot hyvin yleisellä tasolla, tarkemmat laite- ja ohjelmistolistaukset ovat sisällytetty jatkuvuussuunnitelmaan.

Fyysiset laitteet

Virtuaali-infrastruktuuria ylläpitävä fyysinen laiteympäristö koostuu kolmesta virtuaali-isäntäpalvelimesta, näille yhteisestä levyjärjestelmästä sekä kahdennetuista kytkimistä jotka hoitavat liikenteen sekä fyysisten palvelimien ja levyjärjestelmän välillä että myös käyttäjien ja muiden järjestelmien välillä. Palvelimet on mitoitettu kattamaan toistaiseksi nähtävissä oleva tehontarve joustovaraa unohtamatta sekä myös kestämään yhden kokonaisen palvelimen tai kytkimen rikkoontuminen. Keskitetty verkkolevyjärjestelmä on myös hyvin vikasietoinen ja helposti laajennettavissa.

Virtuaaliympäristöä tukemassa ovat lisäksi kahdennettu palomuuri, UPS-järjestelmä vara-akulla sekä nauhakirjasto erillisellä varmuuskopiointipalvelimella. Kuviossa 10 on esitetty yksinkertaistettu kuva laitteistoympäristöstä.

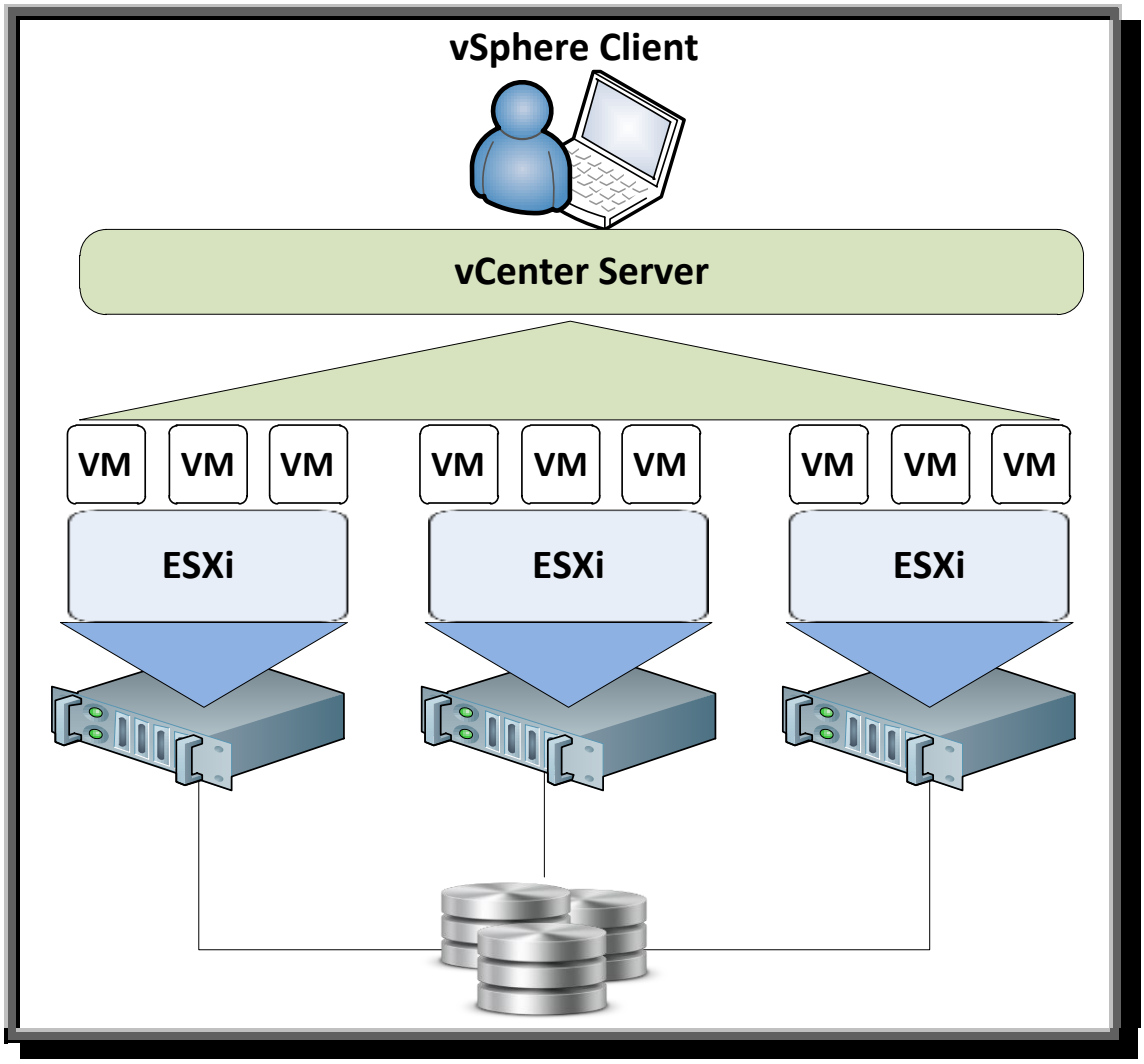


Kuvio 10. Kuva laitteistoympäristöstä

Virtuaaliympäristö

Fyysisten palvelimien ja keskitetyn levyjärjestelmän päälle rakennettu VMWare vSphere 4.1-virtuaaliympäristö tarjoaa joustavan ja vikasietoisen ympäristön yrityksen sisäisille palveluille ja kehitystyölle. Järjestelmä koostuu fyysisille palvelimille asennetuista ESXi-virtualisointisovelluksista, joita hallinnoidaan keskitetysti virtuaaliympäristön sisään asennetulta vCenter-palvelimelta. Järjestelmän etuja ovat mm. palvelinten pohja-asennus, josta on helppo ja nopea kopioida valmiita palvelininstansseja tarpeen mukaan. Virtuaalipalvelimia voidaan myös liikuttaa järjestelmässä isännältä toiselle ilman käyttökatkoja, mikäli törmättäisiin resurssiongelmiin yksittäisellä isäntäpalvelimella. Virtuaaliympäristö mahdollistaa myös sisältämiensä palvelimien ja palveluiden turvallisen päivittämisen ja testaamisen snapshot-ominaisuudella, jonka avulla voidaan päivitystä edeltävästä hetkestä ottaa levykuva palvelimesta. Levykuvan avulla saatetaan helposti palauttaa virtuaalipalvelin päivitystä edeltävään hetkeen, mikäli ongelmiin törmätään.

Ympäristöä hallinnoidaan omalla asiakasohjelmistollaan vCenter-palvelimen kautta, joka pitää kirjaa ympäristön tapahtumista ja historiasta jolloin tarvittaessa saadaan kattavia raportteja virtuaalipalvelimien ja – isäntien suorituskyvystä. Virtuaaliympäristö on kuvattu oheisessa kuvassa 11.



Kuvio 11. VMWare vSphere virtuaaliympäristö

7 Jatkuvuussuunnitelma

Itse jatkuvuussuunnitelma luotiin dokumenttikokoelmaksi ryhmätapaamisissa ja ideariihissä syntyneiden muistioiden perusteella. Tapaamisissa käytiin läpi edellä kuvattuja työvaiheita joiden pohjalta dokumentaatio rakennettiin.

Tässä kappaleessa on kuvattu jatkuvuussuunnittelussa käytettyjä keinoja, dokumenttipohjia ja ohjeistuksia.

7.1 Koordinointi, vastuutus ja dokumentaatio

Yrityksen koosta johtuen osallisina suunnitelman laatimisessa olivat itseni lisäksi vain yrityksen toimitusjohtaja sekä varamieheni joka toimi samalla käyttäjänäkökulmaa tarjoavana resurssina sekä ”koekaniinina” palautumissuunnitelmien toimivuuden ja ymmärrettävyyden suhteen. Päävastuu suunnitelman laatimisessa ja dokumentoinnissa oli allekirjoittaneella.

Suunnittelu tehtiin ideariihityyppisesti edellä mainitun ryhmän tapaamisissa joissa pohdittiin järjestelmiä mahdollisesti uhkaavia todennäköisimpiä riskejä jotka arvotettiin pisteyttämällä. Pisteyttämisen jälkeen varteenotettavimmille riskeille luotiin käsittely- ja palautumissuunnitelmat.

Dokumentaatiossa käytettiin mahdollisimman pitkälti valmiita ja koeteltuja pohjia (esim. VAHTI-ohjeistus), joita osin muokattiin omaan käyttöön sopiviksi mutta myös kokonaan omia dokumenttipohjia luotiin.

7.2 Kriittisten prosessien tunnistaminen ja kuvaaminen

Yrityksen kriittisten prosessien tarkempaa läpikäymistä ei jatkuvuussuunnitelman tässä vaiheessa katsottu vielä tarkoituksenmukaiseksi koska suunnitelman ensimmäinen versio koskee taustajärjestelmää kokonaisuudessaan. Käytännössä kaikki fyysisiin laitteisiin kohdistuvat vakavat häiriöt vaikuttavat myös kaikkiin ympäristön palveluihin joten tarkempiin järjestelmä- tai prosessikuvauksiin ei ollut syytä mennä vielä suunnitelman tässä vaiheessa.

Suunnitelman seuraavassa versiossa keskitytään lähemmin järjestelmän ylläpitämiin palvelimiin ja palveluihin, niihin kohdistuviin riskeihin ja niistä toipumiseen. Suunnitelman seuraavan version työvaiheet ovat kirjattu jatkuvuussuunnitelman päivityssuunnitelmaan.

7.3 Riskien tunnistaminen ja arviointi

Riskien tunnistamisessa käytiin läpi yleisimpiä laitetilaan ja yhteyksiin mahdollisesti vaikuttavia uhkia ja määriteltiin niiden todennäköisyys karkealla tasolla. Määrittelyissä käytettiin hyväksi oheista VAHTI-ohjeistuksessa esiteltyä taulukkoa(2003, 41–42):

Taulukko 1. Uhan todennäköisyyden arviointi (VAHTI 2003, 41–42)

Todennäköisyys	Pisteet	Määritelmä
Korkea	3	Toiminto tai järjestelmä on heikosti valvottua Toimintoon tai järjestelmään pääsy on helppoa Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa Toiminnon ohjeistusta ei ole Tapahtuma ilmenee kerran kuukaudessa Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä
Keskimääräinen	2	Toiminto on osittain valvottua Toiminnon ohjeistus on puutteellista Tapahtuma ilmenee 1–2 kertaa vuodessa Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille
Alhainen	1	Toiminto on hyvin valvottua ja siihen pääsy on hallittua. Toiminto on hyvin ohjeistettu Toimintoa kohtaan ei ole mielenkiintoa Tapahtuma ilmenee kerran vuodessa Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille

Merkityksetön	0	Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

7.4 Vaikutusanalyysi

Vaikutusanalyysissä pohdittiin esilletulleiden uhkien seurauksia ja pisteytettiin niitä karkeasti taulukossa 2 esitellyn VAHTI-ohjeistuksen mukaisen riskien seurausten määrittelytaulukon mukaisesti:

Taulukko 2. Seurausten vakavuuden luokittelu (VAHTI 2003, 42–43)

Vakavuus	Pisteet	Määritelmä
Korkea	3	Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen
Keskimääräinen	2	Seurauksilla on vaikutuksia organisaation sisällä Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) Uhkan toteutuminen aiheuttaa tiedotteen tekemisen Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
Alhainen	1	Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä

		Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä Uhkan toteutuminen aiheuttaa sisäisen raportoinnin Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia Toiminnan keskeytyminen on muutaman minuutin pituinen

Riskin suuruutta arvioitiin vertaamalla selvitetyn riskin vakavuutta sen todennäköisyyteen VAHTI-ohjeistuksessa(2003, 43) esitellyn taulukon (Taulukko 3) mukaan:

Taulukko 3. Riskin suuruuden määrittely (VAHTI 2003, 43)

Kriittisyys		**Seurausten vakavuus**		
		Vähäinen (1)	**Vakava (2)**	**Erittäin vakava (3)**
Uhan todennäköisyys	Korkea (3)	3. Kohtalainen	4. Merkittävä	5. Sietämätön
	Keskimääräinen (2)	2. Vähäinen	3. Kohtalainen	4. Merkittävä
	Alhainen (1)	1. Merkityksetön	2. Vähäinen	3. Kohtalainen

Analyysin tulokset vedettiin yhteen taulukkoon johon on listattu selvityksessä ilmitulleet järjestelmiä uhkaavat riskit ja niiden pisteytykset. Iivari & Laaksonen (2009, 136–137) esittävät yksinkertaisen mutta käytännöllisen pohjan johon riskit saatettiin kootusti kerätä. Taulukkoon (Taulukko 4) nimettiin havaitut riskit ja kirjattiin sanallisesti riskin mahdolliset vaikutukset sekä niille määritetyt pisteet. Lisäksi taulukkoon kirjattiin karkealla tasolla riskin torjunnan mahdollisuus ja sen tämänhetkisen torjunnan taso.

Taulukko 4. Esimerkki Riskitaulukosta (Iivari & Laaksonen 2009, 136-137)

Riski	Vaikutus	Toden-näköisyys	Vaka-vuus	Riskipis-teytys	Torjunta mah-dollista	Torjunta toteu-tettu
Riski A		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain
Riski B		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain
Riski C		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain
Riski D		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain
Riski E		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain
…		n	n	n	kyllä/ei/osittain	kyllä/ei/osittain

7.5 Riskien torjunta ja vaikutusten pienentäminen

Havaitut riskit avattiin sanallisesti omaan taulukkoonsa jossa esitellään riski, toimenpiteet riskin käsittelemiseksi sekä siitä palautumiseksi. Iivari & Laaksonen(2009, 137) antavat myös tähän oman taulukkopohjansa (Taulukko 5):

Taulukko 5. Riskin käsittely (Iivari & Laaksonen 2009, 137)

Riski	
Riskipisteytys	
Todennäköinen skenaario	
Häiriintyneet toiminnot	
Toimenpiteet normaalitilaan palaamiseksi	1. 2. 3. 4. n.
Vastuuhenkilöt	1. 2.
Uhan torjunta	1. 2. 3. 4. n.
Rajoitteet	
Resurssit	

Kuviossa 12 on esimerkki täytetystä riskin käsittelytaulukosta, kuvasta on häivytetty henkilöihin ja resursseihin liittyvät yksityiskohdat.

Riski	Lyhyt sähkökatko		
Riskipisteytys	**Todennäköisyys**	**Vakavuus**	**Riskipisteet**
	2	1	3
Todennäköinen skenaario	Toimitilojen tai rakennuksen sähkönsyöttö katkeaa väliaikaisesti		
Häiriintyneet toiminnot	Suoraan sähköverkossa kiinni olevat laitteet ja virtalähteet (ks. taulukko) Palvelintilan jäähdytys/ilmastointi		
Toimenpiteet normaalitilaan palaamiseksi	1. häiriön vakavuuden selvitys - huoltoyhtiön numero - sähköyhtiön numero 2. häiriintyneiden laitteiden ja toimintojen tarkistus 3. hätäilmanvaihdon järjestäminen 4. UPS:n tilan tarkastus, virran riittävyys katkon ajaksi 5. palvelimien ja laitteiden alasajo hallitsemattoman kaatumisen estämiseksi katkon pitkittyessä, ks. laitteiden sammutus/käynnistysjärjestys 6. katkon päätyttyä laitteiden ja palvelimien käynnistys, ks. järjestystaulukko 7. fyysisten laitteiden tarkastus vahinkojen varalta 8. palveluiden toiminnan tarkastus		
Vastuuhenkilöt	1. 2.		
Uhan torjunta	1. UPS 2. vartiointiliike, hälytys sähkökatkosta toimistoajan ulkopuolella		
Rajoitteet	UPS:n akusto henkilökunnan paikallaoloajat		
Resurssit	UPS vastuuhenkilöt huoltoyhtiö sähköyhtiö		

Kuvio 12. Esimerkki täytetystä riskin käsittelytaulukosta

8 Varautumistoimenpiteet

Järjestelmän jatkuvuuteen ja saavutettavuuteen kiinnitettiin huomiota jo rakennusvaiheessa, tässä luvussa käsitellään toimenpiteet ja järjestelmät joilla mahdollisiin ongelmatilanteisiin on pyritty varautumaan tai tunnistamaan ne etukäteen.

Laitteistoturvallisuus

Jokainen ympäristön laite on haavoittuvilta osiltaan vähintään kahdennettu ja fyysisille palvelimille on asennettu ainoastaan VMWare ESXi-ohjelmisto RAID1-peilatuille levyille. Palvelimilta löytyy useampi verkkokortti jotka on yhdistetty toimimaan niin kuormaa tasaavasti kuin myös vikasietoisuutta tarjoavasti. Palvelimien ja levyjärjestelmien virtalähteet on kahdennettu.

Ympäristön kytkimet on niin ikään kahdennettu, yhden kytkimen rikkoutuminen ei vielä kaada järjestelmää mutta saattaa osin hidastaa toimintaa. Järjestelmä on suojattu virtapiikeiltä ja virran katkeamiselta UPS-laitteistolla joka antaa virtaa n. 20 minuutin ajan virran katkettua mahdollistaen toimimisen lyhyen sähkökatkon aikana tai palvelimien turvallisen alasajon pidemmän sähkökatkon tapahtuessa. Kahden virtalähteen omaavat laitteet on kytketty toisella johdolla UPS-laitteistoon ja toisella suoraan verkkovirtaan jolla pyritään välttämään mahdollinen UPS-laitteiston rikkoutumisesta johtuva järjestelmien hallitsematon kaatuminen.

Kaikki virtuaalipalvelintiedostot sisältävä NetApp-levyjärjestelmä käyttää omaa RAID6:sta jatkettua RAID-DP-tekniikkaansa joka sallii kahden levyn rikkoutumisen ennen datahävikkiä, lisäksi levypakalle on määritelty tyhjä spare-levy joka otetaan käyttöön levyrikon sattuessa, joten yhteensä järjestelmä kestää kolmen levyn rikkoutumisen yhden vuorokauden sisällä. Levyjärjestelmän virransyöttö sekä verkkoyhteydet on niin ikään kahdennettu.

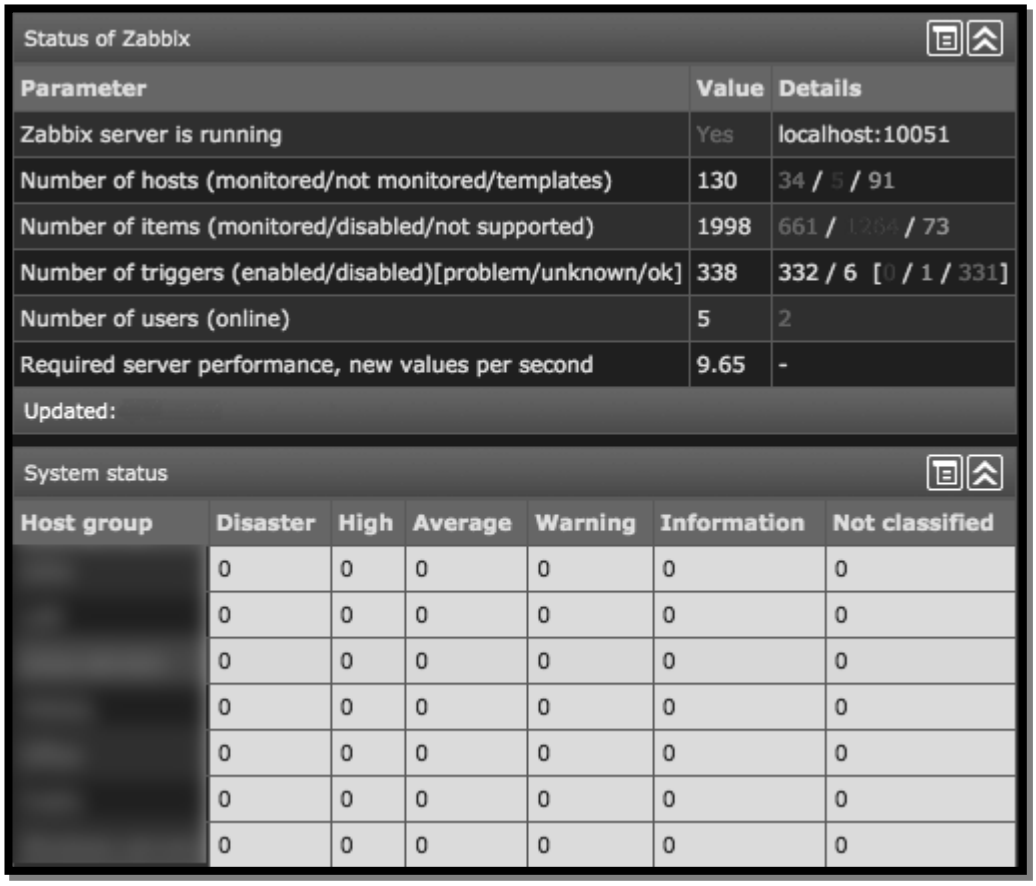
Klusterointi

Virtuaaliympäristö on rakennettu klusteroiduksi VMWare vSphere 4.1 virtualisointituoteperheen tuotteilla. Ympäristö koostuu kolmesta ESXi-virtuaali-isäntäpalvelimesta joiden vikasietoisuus on toteutettu HA-klusteroinnilla(High Availability). Virtuaali-

isännän vikaantuessa siirtyvät automaattisesti tämän sisältäneet virtuaalipalvelimet toimivalle isäntäpalvelimelle ja käynnistyvät uudelleen. Täten yhden isäntäpalvelimen vikaantuminen ei vielä kaada koko ympäristöä.

Valvonta

Virtuaalipalvelimien valvonta on toteutettu pääosin Zabbix-verkonhallintaohjelmalla. Palvelimiin on asennettu agenttipalvelu, jonka kautta Zabbix tekee kyselyitä esim. prosessorikuormasta, levytilasta jne. Hallintaohjelmassa on määritetty raja-arvot joiden - tapauksesta riippuen - alittuessa tai ylittyessä lähetetään hälytyssähköposti kahden tunnin välein määritellyille henkilöille tai postituslistoille kunnes tilanne on korjattu. Kuviossa 13 on ruutukaappaus Zabbixin valvomien palvelimien ja palveluiden yleiskuvasta josta yhdellä katsauksella voi nähdä mahdolliset ongelmatilanteet. Kuviosta on häivytetty valvottuun ympäristöön liittyvät yksityiskohdat.



Status of Zabbix

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (monitored/not monitored/templates)	130	34 / 5 / 91
Number of items (monitored/disabled/not supported)	1998	661 / 1264 / 73
Number of triggers (enabled/disabled)[problem/unknown/ok]	338	332 / 6 [0 / 1 / 331]
Number of users (online)	5	2
Required server performance, new values per second	9.65	-

Updated:

System status

Host group	Disaster	High	Average	Warning	Information	Not classified
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0
[redacted]	0	0	0	0	0	0

Kuvio 13. Zabbix-valvontajärjestelmän yleiskatsaus

Myös valvontajärjestelmä on osin kahdennettu: ulkoiseen laitetilaan on asennettu vastaava Zabbix-valvontajärjestelmä joka valvoo yrityksen tiloissa olevia julkisia palveluita

ja osaa palvelimista. Mikäli yrityksen sisä- tai ulkoverkko jostain syystä halvaantuisi eikä sisäinen valvontajärjestelmä täten voisi lähettää hälytyksiä, lähettää ulkoinen valvontapalvelin hälytyksen sekä ulkoiseen sähköpostiosoitteeseen että tekstiviestitse asianomaisille henkilöille.

Virtuaaliympäristön vCenter-hallintapalvelin osaa myös tarkkailla ympäristön tilaa niin virtuaali- kuin isäntäpalvelimien osalta ja on myös konfiguroitu lähettämään hälytyssähköposteja vikatilanteen ilmaantuessa. Myös muiden yksittäisten laitteiden mahdolliset sisäiset hälytysjärjestelmät ovat konfiguroitu ilmoittamaan, mikäli laite havaitsee itsessään vikoja.

Ulkoverkko

Yhteydet maailmalle on osin kahdennettu. Mikäli primäärinen kuituyhteys katkeaa, voidaan siirtyä käyttämään erillistä kaapeliyhteyttä yksinkertaisella reititysmuutoksella. Kaapeliyhteys toimii kuitenkin vain käyttäjien väliaikaisena yhteytenä ulkomaailmaan, esim. palvelimia ei saa varaverkosta näkymään maailmalle koska palvelimien julkiset osoitteet sijaitsevat ainoastaan ensisijaisessa verkossa.

Suojaus

Verkon suojaus on toteutettu kahdennetulla open source-palomuuriratkaisulla. Palvelimet, käyttäjät ja laitteet on eroteltu omiin virtuaalilähiverkkoihinsa(VLAN) joiden välinen sallittu liikenne määritellään palomuuriasetuksilla, lähtökohtana vain tarvitut sallitut portit ja protokollat kuhunkin suuntaan verkkojen välillä. Active Directory-käyttäjähallinnan avulla ylläpitopääsy palvelimille on sallittu vain nimetyille henkilöille, joille on annettu erillinen ylläpitotunnus.

F-Secure virustorjunta on asennettu tiedostopalvelimelle, sähköpostipalvelimelle sekä kaikkiin työasemiin. Virustorjuntaa seurataan ja ylläpidetään keskitetysti F-Secure Policy Manager-ohjelmistolla joka päivittää virustunnisteet sekä hälyttää sähköpostitse mikäli tietokoneilla havaitaan virustartuntoja tai -hyökkäyksiä.

Itse fyysiset palvelimet ja laitteet sijaitsevat yrityksen toimitiloissa lukitussa tilassa johon on avaimet vain nimetyillä henkilöillä. Itse toimitilat on kattavasti suojattu luvattomalta

tunkeutumiselta liikeilmaisimilla jotka hälyttävät vartiointiliikkeeseen mikäli tiloissa havaitaan liikettä toimitilojen ollessa tyhjillään. Palvelinhuone on myös ilmastoitu ja jäähdytetty ja tilaan on myös asennettu lämpötilahälytin joka tekee hälytyksen vartiointiliikkeeseen, mikäli palvelintilan lämpötila nousee liian korkeaksi jolloin huoneeseen järjestetään hätäilmastointi ohjeistuksen mukaisesti vikatilanteen ajaksi.

Huoltosopimukset

Järjestelmän kaikille laitteille on olemassa kattava huoltosopimus, joka takaa laitteistorikkojen tapahtuessa laitteiden huollon ja vikaantuneiden komponenttien vaihdon seuraavan työpäivän kuluessa.

8.1 Varmuuskopiointi

Päävarmuuskopiointimetodiksi Yritys X:n järjestelmille valikoitui ympäristöä rakennettaessa LTO4-nauhavarmistus erillisen varmuuskopiointiohjelman ohjaamana. Valintaan vaikutti varmistusten helppo säilytys ja siirrettävyys sekä myös luonnollisesti kustannustekijät. Nauhavarmistusten lisäksi levyjärjestelmässä on käytössä automaattinen snapshot-ominaisuus, joka tallentaa kaikkien virtuaalikoneiden tilan ja datan määritellyin aikavälein. Lisäksi osalla virtuaalipalvelimista on paikallisia varmuuskopiointirutiineja tietokannoille ja dokumenteille.

Nauhavarmistukset

Koska virtualisoidun IT-infrastruktuurin kaikki järjestelmät ja tiedostot sijaitsevat keskitetyllä levyjärjestelmällä, katsottiin tehokkaimmaksi ratkaisuksi hoitaa varmuuskopiointi suoraan levyjärjestelmältä nauhoille ilman virtuaalipalvelimille asennettavia agentteja. Tällä tavoin jokaisella varmistuskierrolla varmistetaan koko ympäristö kaikkine palvelimineen ja asetuksineen. Datamäärät tällä varmistusmetodilla ovat verrattain korkeat, mutta testien mukaan ajallisesti sekä nauhojen kulutuksen suhteen nähtävissä olevassa tulevaisuudessa valittuun tapaan soveltuvat. Nauhojen kiertosuunnitelma on kuvattu oheisessa taulukossa 6.

Taulukko 6 Nauhojen kiertosuunnitelma

Nauha	**Päivä**	**Kuukausi**	**Vuosi**
Frekvenssi	ma, ke, pe	joka kuukauden 1. lauantai, pl. vuosi-nauhojen ottopäi-vät	tammikuun 1. lauantai heinäkuun 1. lauantai
Säilytysaika	14 pv	6 kk	∞
Säilytyspaikka	Dataturvakaappi	off-site	tallelokero
Nauhojen tarve	6x nauhakulutus per backup	5x nauhakulutus per backup	2x nauhakulutus per backup per vuosi

Nauhoista otetaan kolmea säilytysajaltaan erilaista tyyppiä, joihin kaikkiin kuitenkin sisällytetään koko levyjärjestelmän sisältö. Päivänauhoja säilytetään kaksi viikkoa toimitiloissa sijaitsevassa koodilukollisessa dataturvakaapissa, kuukausinauhoja puoli vuotta toimitilojen ulkopuolella ja puolivuosittain otettavat kertakirjoitettavat WORM-nauhat säilytetään ”ikuisesti”, kuitenkin vähintään 2 vuotta pankin tallelokerossa.

Snapshot

Käytössä olevan levyjärjestelmän NetApp FAS 2040 ominaisuuksiin kuuluu automaattinen snapshot-kierto, joka määritellyin välein ottaa kaikesta levyjärjestelmän datasta levykuvan. Taulukossa 7 on kuvattu snapshotien kierto. Snapshot-ominaisuus ei tarjoa turvaa levyjärjestelmän rikkoutumiselle, mutta on apuna jos virtuaalipalvelimen toiminnassa tai datassa tapahtuu häiriöitä jotka havaitaan nopeasti.

Taulukko 7. Levyjärjestelmän snapshot-kierto

Snapshot	Hourly	Nightly	Weekly
Aika	klo 8, 12, 16, 20	ma-su klo 24.00	sunnuntaisin klo 24.00
Säilytysaika	1 vrk	2 vrk	1 vko

Paikalliset varmuuskopiot

Pääosin tietokantapalvelimille on määritetty paikallisia varmuuskopiointirutiineja, jotka säilyttävät dataa paikallisesti virtuaalikoneissa. Paikalliset varmuuskopiot on tarkoitettu lähinnä sovellusten pääkäyttäjille, jotka voivat itsenäisesti palauttaa dataa mikäli havaitsevat ongelmia. Kierto paikallisissa varmuuskopioissa pidetään lyhyenä(1-2 päivää), koska pidempään jatkunut tilanne voidaan aina palauttaa nauhavarmistuksista ja tällä tavoin vähennetään turhan datamassan kertymistä.

Dokumenttipalvelimella on lisäksi käytössä Shadow Copy-ominaisuus, joka säilyttää versiohistoriaa tallennetuista dokumenteista ja antaa käyttäjille mahdollisuuden palauttaa itsenäisesti vahingossa tuhottuja tai virheellisesti muokattuja tiedostoja Windowsin ”Previous Versions” -toiminnon avulla.

Palautustestaus

Palautustestaus suoritetaan joka kolmannen kuukauden ensimmäisen viikon aikana, tarkoituksena selvittää seuraavat asiat:

- varmuuskopioitava data todella menee nauhoille
- nauhoille menevä data on eheää
- tiedostot ovat löydettävissä nauhoilta
- data on palautettavissa levyjärjestelmään
- palautettava data on eheää ja käyttökelpoista
- palautuksen ohjeistus on riittävän selkeä ja ajantasainen
- asianomaiset osaavat suorittaa palautuksen ohjeistuksen mukaisesti

Palautustestausprosessissa testataan sekä päivä- että kuukausinauhoilta palauttaminen. Päivänauhoilta palautetaan satunnainen yksittäinen tiedosto, esim. asennuslevyn image.

Kuukausinauhoilta palautetaan kokonainen virtuaalikone kaikkine tiedostoineen, tarkistetaan että palvelin käynnistyy ja sen tila vastaa nauhallekirjoitushetkeä. Tarkempi palautustestausprosessi on kuvattu jatkuvuussuunnitelmassa.

8.2 Suunnitelmien dokumentointi, testaus ja ylläpito

Edellä esitellyt arviot, suunnitelmat ja taulukot koostettiin yhtenäiseksi dokumenttikokoelmaksi jota säilytetään digitaalisesti ja fyysisesti kahdessa eri lokaatiossa, lukituissa säilytystiloissa.

Järjestelmäkuvausdokumentti (Liite 1)
Edellä kuvattujen taulukoiden lisäksi luotiin järjestelmäkuvausdokumenttipohja eri järjestelmien ja järjestelmäkokonaisuuksien kokonaiskuvaukseen. Järjestelmäkuvausdokumenttiin kerätään mahdollisimman tarkat tiedot järjestelmäkokonaisuudesta, sen osista ja suhteista sekä yhteyksistä muihin palveluihin. Järjestelmäkuvausdokumentti toimii myös osin ylläpitodokumenttina loppuosan toimintaohjeiden ja case-kuvausten avulla ja sitä tulisikin ylläpitää myös normaalin päivityssyklin ulkopuolella. Dokumentti havaittiin valmistuttuaan hyödylliseksi myös projektityössä käytettäväksi ja halusipa erään asiakkaan käyttöpalveluntarjoajakin dokumenttipohjan käyttöönsä.

Säilytys ja päivittäminen
Jatkuvuussuunnitteludokumentaatiota säilytetään sekä sähköisessä että fyysisessä muodossa, ja vähintään yhdessä erillisessä fyysisessä sijainnissa toimitilojen ohella(vielä auki tätä kirjoitettaessa). Toimitiloissa dokumentaatiota säilytetään palo- ja murtoturvallisessa dataturvakaapissa ja erillisessä sijainnissa lukitussa tilassa. Jatkuvuussuunnitteludokumentaation fyysiset kopiot koostetaan yhtenäisiksi kansioiksi joiden ensimmäiselle lehdelle lisätään dokumentaation versiohistoria, säilytyspaikat sekä dokumentaation ylläpidosta vastuulliset henkilöt.

Dokumentaatio tarkastetaan ja päivitetään vuosittain helmikuun aikana. Tarkastuksen yhteydessä käydään läpi vähintään seuraavat asiat:

- vastuuhenkilöt
- laitteistoinventaario, tukisopimukset
- toipumissuunnitelmien ajantasaisuus

Dokumentin versiohistoriaan kirjataan muutokset, niiden tekijät sekä seuraavan tarkastuksen ajankohta.

9 Yhteenveto

Lopputyön tavoitteena oli luoda yritykselle helposti ymmärrettävä ja ylläpidettävä dokumentaatiopohja yrityksen IT-infrastruktuurista, siihen mahdollisesti kohdistuvista riskeistä ja kuinka niihin on varauduttu. Lopputyön aihe valikoitui osin yrityksen ulkoisiin vaatimuksiin vastaamiseksi, mutta suoritetta tehdessä nopeasti selvisi kuinka hyödyllisestä ja tarpeellisesta asiasta olikaan kyse. Aikanaan itse järjestelmää rakennettaessa ei pohjalla ollut varsinaista opiskeltua teoriapohjaa jatkuvuussuunnittelusta mutta lähdemateriaaleihin tutustuessa havaitsin että jo rakennusvaiheessa oli paljon asioita tehty oikein ilman opaskirjojakin.

Aiheen rajauksessa jouduin hieman käyttämään pohdintaa, mitä olisi tarkoituksenmukaisinta sisällyttää suunnitelman tähän vaiheeseen. Päädyin käsittelemään ainoastaan taustajärjestelmiä koska kaikki palvelut ja prosessit ovat loppujen lopuksi riippuvaisia fyysisten laitteiden toiminnasta ja näihin kohdistuvat häiriöt vaikuttavat kaikkeen toimintaan. Suunnitelmaa kirjoittaessa ei varsinaisiin yllätyksiin törmätty vaan asioiden kirjaaminen sujui suhteellisen kivuttomasti. Kaikki tieto oli jo olemassa allekirjoittaneen päässä, lähdemateriaaleja ja ryhmätapaamisia käyttäen tämä tieto saatiin kirjattua strukturoituun ja myös muille ymmärrettävään muotoon. Tiedon leviäminen yrityksen sisällä oli myös yksi ehdottoman positiivisista tuloksista joka suunnitelman tekemisestä seurasi.

Lopputyön tuloksena syntyneet dokumentit ja pohjat pyrittiin tekemään mahdollisimman helposti ymmärrettäviksi ja päivitettäviksi, jossa tavoitteessa onnistuttiin mielestäni erittäin hyvin. Pyörää ei ollut syytä lähteä keksimään uudelleen koska lähdemateriaaleista löytyi rutkasti valmiita ja koeteltuja pohjia arvioinneille ja kirjauksille. Oman työn tuloksena syntynyt dokumenttipohja järjestelmäkuvauksille osoittautui myös erittäin käyttökelpoiseksi ja se otettiin käyttöön yrityksessä yleisemminkin.

Itse jatkuvuussuunnitelmassa on vielä rutkasti kehitettävää ja kuten aiemmin on mainittu, jatkuvuussuunnittelu on jatkuva prosessi. Tästä lopputyöstä syntynyt dokumentaatio onkin vasta suunnitelman ensimmäinen vaihe joka pidettiin tarkoituksella laaja-alaisena.

Suunnitelman seuraavilla tarkastus- ja päivityskierroksilla pureudutaan tarkemmin itse liiketoiminnan prosesseihin ja niitä tukeviin palveluihin.

Ammatillisesti opinnäytetyön tekeminen opetti paljon jatkuvuuteen ja varautumiseen liittyvästä suunnittelusta ja järjestelmällisestä riskeihin varautumisesta. Tehdyille asioille ja kirjaamattomille suunnitelmille löytyi nimiä ja käsitteitä sekä malleja joiden pohjalta suunnittelun jatkamista ja kehittelyä on helppo edistää. Myös tiedon leviäminen parantaa selvästi yrityksen valmiutta mahdollisiin ongelmatilanteisiin ja yleisesti ottaen ymmärrystä yrityksen järjestelmien toiminnasta.

Lähteet

Laaksonen, M., Nevasalo, T. & Tomula K. 2006. Yrityksen tietoturvakäsikirja. Edita. Helsinki.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo. Porvoo.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. 2009. Tietosanoma. Tallinna.

VAHTI 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf. Luettu 12.3.2012

Jordan, E., Silcock, L. 2006. Strateginen IT-riskien hallinta. Edita. Helsinki

Tietotekniikan Liitto RY 2007. PK-yritysten tietoturvakysely. Luettavissa: http://www.ttlry.fi/tutkimus/pk-tietoturvatutkimus. Luettu 10.5.2012

EMC 2011. European Disaster Recovery Survey. Luettavissa: http://emea.emc.com/collateral/microsites/2011/emc-brs-survey/european-disaster-recovery-survey-2011.pdf. Luettu 22.3.2012

Liitteet

Liite 1. Järjestelmäkuvausdokumentti

1 PERUSTIEDOT

1.1 Vastuuhenkilöt

1.1.1 Yritys X

Rooli	Nimi	Sähköposti	Puhelin
Järjestelmävastaava			
Sovellusvastaava			
Varamies 1			
Varamies 2			

1.2 Informointi

Keille kaikille tulee informoida, missä tilanteissa ja millä yhteydenottomenetelmällä

2 PALVELIMET

2.1 <Palvelin 1>

<Lyhyt kuvaus palvelimen tehtävästä ja palveluista>

2.1.1 Laitteisto

Palvelimen nimi	
Valmistaja	
Malli	
Prosessori (asennettu/kannat)	
Muisti	
Verkkokortit	
Huoltosopimus	

viim. voimassaolopäivä	
Kiintolevyt	
Malli, määrä	
RAID-konfiguraatio	
Nettokiintolevytila	

2.1.2 Ohjelmistot

Käyttöjärjestelmä	
Lisensoidut ohjelmistot	
Palvelut	
Sovellus	

2.1.3 Verkkoasetukset

IP-osoitteet	
DNS-nimi	
Gateway	
Verkko	
DNS-palvelimet	
Reitit	

2.1.4 Yhteydet muihin palveluihin

Palvelu	**Palvelin**	**Kuvaus**

2.1.5 Tunnukset

Käyttötarkoitus	**Tunnus**	**Salasana**

2.1.6 Ylläpitoskriptit & ajastetut tehtävät

Käyttötarkoitus	**Sijainti**	**Ajastus**

2.1.7 Logitiedostot

Sovellus	**Sijainti**	**Kierto**

2.1.8 Muuta tietoa

Muu tarpeellinen tieto palvelimesta tai siihen liittyvistä asioista

3 VERKKOYMPÄRISTÖ

3.1 Tietoverkkokuvaus

<visiokuva, lyhyt selite ympäristöstä, verkkoympäristön palvelimet>

3.2 Palomuurisäännöt

Lähteen ip-osoite	**Kohteen ip-**	**Portti/protokolla**	**Selite**

tai verkko	osoite tai verkko		

4 VARMUUSKOPIOINTI

Lyhyt yleiskuvaus varmuuskopioista

- mitä tietoja kopioidaan
- minne tiedot kopioidaan(paikalliset & ulkoiset varmuuskopiot)
- millä kopioidaan

4.1 Kopioitavat tiedostot ja kansiot

Tarkempi erittely kopioitavista kohteista

4.2 Varmuuskopiokäytännöt

- rutiinit (päivä/viikko/kuukausi)
- tallennusmetodi
- säilytysaika

4.3 Palautustestaus

5 YLEISET OHJEET

5.1 Ylläpitoyhteys

(Kuvallinen) Step-by-step –ohjeistus yhteyden ottamisesta palvelimille:

- yhteydenottotapa (SSH/RDP)
- mahdolliset VPN-asetukset
- osoite/portti
- tunnukset

5.2 Palveluiden käynnistysohjeet

5.2.1 <Palvelin 1>

(Kuvallinen) Step-by-step –ohjeistus palveluiden käynnistämiseksi

5.3 Palveluiden sammutusohjeet

5.3.1 <Palvelin 1>

(Kuvallinen) Step-by-step –ohjeistus palveluiden käynnistämiseksi. Palveluiden toimivuuden tarkistusohjeet

5.4 Muut yleiset ohjeet

Tapauskohtaisesti

- tiivistelmä(mitä on tarkoitus tehdä)
- mitä teen
- miten tarkistan
- (kuvalliset) step-by-step -ohjeet

6 FAQ

Tähän osioon kerätään palvelimilla/palveluissa havaitut (toistuvat) ongelmat ratkaisukuvauksineen ja step-by-step –ohjeineen

6.1 Case 1

6.2 Case 2